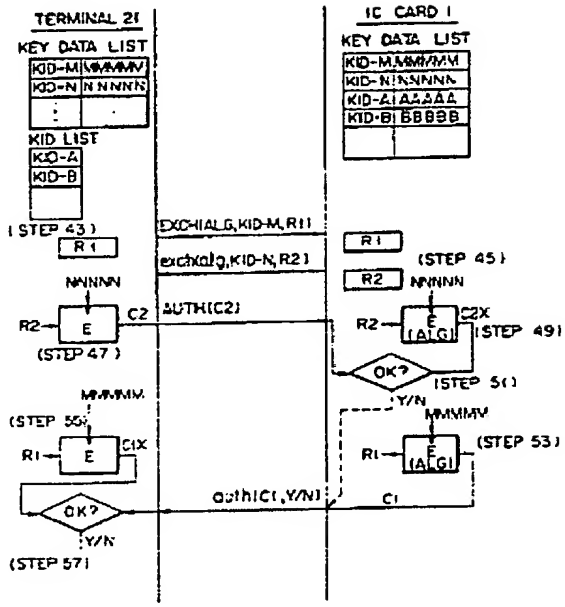
Certification system

Patent number: FR2641885
Publication date: 1990-07-20
Inventor: IIJIMA YASUO
Applicant: TOKYO SHIBAURA ELECTRIC CO (JP)
Classification:
- international: G06K19/07; G09C1/00
- european: G07F7/10D4E2; G07F7/10D10M; G07F7/10E
Application number: FR19900000511 19900117
Priority number(s): JP19890008010 19890117; JP19890008011 19890117

Also published as:
GB2227111 (A)

Abstract not available for FR2641885
Abstract of corresponding document: **GB2227111**

A terminal 21 sends, to a card 1, a random number R1, an encryption algorithm selector number ALG and a key data selector number KID-M, to certify the card and the card sends numbers R2, KID-N to certify the terminal (Fig. 3A). Data from the terminal to be written into the card can be encrypted in the card using R1, ALG and KID-M.



F I G. 3A

Express Label No.
EV343685915US

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 641 885**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **90 00511**

(51) Int Cl[5] : G 06 K 19/07; G 09 C 1/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 17 janvier 1990.

(30) Priorité : JP, 17 janvier 1989, n° 1-8010 et n° 1-8011.

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 29 du 20 juillet 1990.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *Société dite : KABUSHIKI KAISHA TOSHIBA.* — JP.

(72) Inventeur(s) : Yasuo Iijima.

(73) Titulaire(s) :

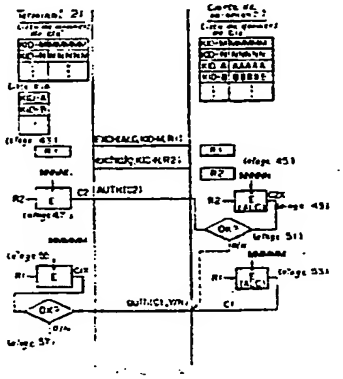
(74) Mandataire(s) : Cabinet Beau de Loménie.

(54) Système de vérification de données pour une carte de paiement.

(57) L'invention concerne les cartes de paiement.

Un terminal 21 désigne une donnée parmi un ensemble de données de clé qui sont conservées dans une carte de paiement 1. Des données à écrire sont cryptées en utilisant la donnée de clé désignée (KID-M). Le terminal désigne une donnée de clé (KID-N) et un algorithme de cryptage alg. Le cryptage des données à écrire s'effectue en utilisant des données, telles qu'un paramètre, dont la valeur change à chaque opération, et la carte de paiement émet les données cryptées vers le terminal. Le terminal vérifie la validité de la carte de paiement avant l'écriture des données dans cette dernière.

Application aux transactions monétaires.



FR 2 641 885 - A1

La présente invention concerne un système et un procédé de vérification ayant pour but de vérifier des données qui doivent être écrites par exemple dans une mémoire dans une carte de paiement ou "carte à puce".

Une attention considérable a été consacrée récemment à un nouveau support d'enregistrement de données portable consistant en une carte de paiement dite carte à puce, qui contient une puce de circuit intégré comprenant une mémoire effaçable non volatile et un élément de commande, tel qu'un microprocesseur, pour commander les composants respectifs, y compris la mémoire.

Dans un système de cartes de paiement classiques utilisant de telles cartes de paiement, comme par exemple un système de paiement d'achats ou un système de crédit, lorsqu'une opération d'écriture de données doit être effectuée en relation avec une carte de paiement (une mémoire dans la carte de paiement), et en particulier lorsque des données de transaction doivent être écrites, les données de transaction qui sont émises vers un centre de traitement (ordinateur hôte) ne peuvent pas être vérifiées au centre de traitement.

Pour cette raison, le système et le procédé de vérification suivants ont été proposés.

Lorsqu'une carte de paiement reçoit une instruction d'écriture de données qui est émise par un terminal, les données à écrire sont cryptées dans la carte de paiement en utilisant des données de clé prédéterminées et un algorithme de cryptage prédéterminé. Une partie des données cryptées est fournie au terminal. Le terminal fournit alors au centre de traitement les données cryptées et les données à écrire. Le centre de traitement vérifie les données à écrire en utilisant les données qui lui sont fournies.

Cependant, dans un tel procédé de vérification, si des cartes de paiement sont utilisées dans plusieurs applications, du fait qu'elles sont de plus en plus utilisées dans divers buts, un moyen efficace pour assurer la sécurité entre les applications respectives consiste à utiliser des données de clé de vérification différentes qui sont conservées dans les applications en vue de la vérification.

Dans le procédé de vérification décrit ci-dessus, si on utilise des données à écrire, des données de clé et des algorithmes de cryptage identiques, une carte de paiement fournit en sortie les mêmes données cryptées. La vérification des données de transaction devient donc difficile.

En outre, dans un tel procédé de vérification, il est nécessaire de mettre en oeuvre des instructions spéciales pour désigner des données de clé et des algorithmes de cryptage qui sont employés pour crypter des données à écrire dans une carte de paiement.

Un but de l'invention est de procurer un système et un procédé de vérification pour un dispositif électronique portable dans lesquels, même si une carte de paiement est utilisée dans plusieurs applications, des données de clé et des algorithmes de cryptage pour la vérification peuvent être utilisés sélectivement pour chaque application, de façon à assurer la sécurité entre les applications.

Un autre but de l'invention est de procurer un système et un procédé de vérification dans lesquels même si des données à écrire, des données de clé et des algorithmes de cryptage identiques sont utilisés, des données cryptées différentes sont émises, à condition que l'instant auquel une opération d'écriture est effectuée ne soit pas le même, ce qui facilite la vé-

rification.

Un autre but de l'invention est de procurer un système de vérification dans lequel il ne soit pas nécessaire d'utiliser des instructions spéciales pour désigner des données de clé et des algorithmes de cryptage utilisés pour crypter des données, ce qui permet de réduire la charge de travail imposée à une carte de paiement.

Un premier aspect de l'invention procure un système de vérification comprenant un premier dispositif électronique contenant au moins une donnée de clé, un second dispositif électronique capable d'entrer en communication avec le premier dispositif électronique, des moyens pour émettre du second dispositif électronique vers le premier dispositif électronique des premières données et des données de désignation pour désigner des données de clé pour le cryptage des premières données, des moyens qui, lorsque les premières données et les données de désignation sont reçues par le premier dispositif électronique, sélectionnent une donnée de clé parmi les données de clé précitées, conformément aux données de désignation reçues, et cryptent les premières données reçues en utilisant la donnée de clé sélectionnée, et des moyens pour émettre une partie des données cryptées vers le second dispositif électronique, après que le premier dispositif électronique a entièrement reçu les premières données.

Un second aspect de l'invention procure un système de vérification comprenant un premier dispositif électronique qui contient au moins une donnée de clé et au moins un algorithme de cryptage, un second dispositif électronique capable d'entrer en communication avec le premier dispositif électronique, des moyens pour émettre du second dispositif électronique vers le premier dispositif électronique des premières

données, des données de clé pour le cryptage des premières données, et des données de désignation pour désigner un algorithme de cryptage, des moyens qui, lorsque les premières données et les données de désignation sont reçues par le premier dispositif électronique, sélectionnent une donnée de clé et un algorithme de cryptage parmi la ou les données de clé et le ou les algorithmes de cryptage, conformément aux données de désignation reçues, et cryptent les premières données reçues en utilisant la donnée de clé et l'algorithme de cryptage sélectionnés, et des moyens pour émettre vers le second dispositif électronique une partie des données cryptées, après que le premier dispositif électronique a entièrement reçu les premières données.

Un troisième aspect de l'invention procure un système de vérification comprenant un premier dispositif électronique qui contient des données de clé et un algorithme de cryptage, un second dispositif électronique capable d'entrer en communication avec le premier dispositif électronique, des moyens pour émettre du second dispositif électronique vers le premier dispositif électronique des premières données et des secondes données dont le contenu varie à chaque opération, des moyens qui, lorsque les premières et secondes données sont reçues par le premier dispositif électronique, cryptent les premières données reçues en utilisant les secondes données reçues, les données de clé et l'algorithme de cryptage, et des moyens pour émettre vers le second dispositif électronique une partie des données cryptées, après que le premier dispositif électronique a entièrement reçu les premières données.

Un quatrième aspect de l'invention procure un système de vérification comprenant un premier dis-

positif électronique qui contient au moins une donnée de clé et au moins un algorithme de cryptage, un second dispositif électronique capable d'entrer en communication avec le premier dispositif électronique; des moyens pour émettre du second dispositif électronique vers le premier dispositif électronique des premières données, des données de clé pour le cryptage des premières données et des données de désignation pour désigner un algorithme de cryptage, des moyens qui, lorsque le premier dispositif électronique a reçu les premières données et les données de désignation, sélectionnent une donnée de clé et un algorithme de cryptage parmi la ou les données de clé et le ou les algorithmes de cryptage, conformément aux données de désignation reçues, cryptent les premières données reçues en utilisant la donnée de clé et l'algorithme de cryptage sélectionnés, et émettent les données cryptées vers le second dispositif électronique, des moyens qui, lorsque le second dispositif électronique a reçu les données cryptées, vérifient le premier dispositif électronique sur la base du contenu des données cryptées reçues, des moyens pour émettre des secondes données du second dispositif électronique vers le premier dispositif électronique, des moyens qui, lorsque le premier dispositif électronique a reçu les secondes données, cryptent les secondes données reçues en utilisant la donnée de clé et l'algorithme de cryptage sélectionnés sur la base des données de désignation; et des moyens pour émettre une partie des données cryptées, du premier dispositif électronique vers le second dispositif électronique.

Conformément à l'invention, le terminal désigne une donnée parmi un ensemble de données de clé qui sont conservées dans la carte de paiement, et des données à écrire sont cryptées en utilisant la donnée

de clé désignée. Par conséquent, même si la carte de paiement est utilisée dans un ensemble d'applications, des données de clé de vérification peuvent être utilisées sélectivement pour chaque application, ce qui garantit la sécurité entre les applications.

De plus, le terminal désigne une donnée de clé et un algorithme de cryptage parmi un ensemble de données de clé et d'algorithmes de cryptage qui sont conservés dans la carte de paiement, et des données à écrire sont cryptées en utilisant la donnée de clé et l'algorithme de cryptage désignés. Par conséquent, même si la carte de paiement est utilisée dans un ensemble d'applications, des données de clé de vérification peuvent être utilisées sélectivement pour chaque application, ce qui garantit la sécurité entre les applications.

En outre, en cryptant des données à écrire par l'utilisation de données dont le contenu varie à chaque opération et qui sont émises par le terminal vers la carte de paiement, des données cryptées différentes sont présentées en sortie à condition que des opérations d'écriture soient effectuées à des instants différents, même si on utilise des données à écrire, des données de clé et des algorithmes de cryptage identiques. La vérification est donc facilitée.

D'autres caractéristiques et avantages de l'invention seront mieux compris à la lecture de la description qui va suivre de modes de réalisation et en se référant aux dessins annexés sur lesquels :

La figure 1 est un schéma synoptique montrant une configuration de système comprenant une carte de paiement, un terminal et un centre de traitement, à laquelle un système de vérification conforme à l'invention est appliqué;

La figure 2 est une représentation montrant

la configuration d'une mémoire 3 dans la carte de paiement de la figure 1;

Les figures 3A à 3C sont des représentations qui montrent une procédure pour une opération de vérification mutuelle entre la carte de paiement et le terminal, et une procédure pour l'écriture de données du terminal vers la carte de paiement;

Les figures 4A à 4G sont des organigrammes destinés à l'explication du fonctionnement de la carte de paiement;

La figure 5 est une représentation montrant un format d'un ordre de préparation de vérification;

La figure 6 est une représentation montrant un format d'un ordre de vérification;

La figure 7 est une représentation montrant un format d'un ordre de préparation de cryptage; et

Les figures 8A et 8B sont des représentations montrant des formats d'un ordre d'écriture.

La figure 1 montre une configuration d'un système qui est constitué par une carte de paiement (premier dispositif électronique), un terminal (second dispositif électronique) qui constitue un dispositif hôte, et un centre de traitement (ordinateur hôte), conforme à l'invention.

Une carte de paiement 1 comprend une mémoire 3 pour enregistrer diverses données, un générateur de nombres aléatoires 5 pour produire des données de nombres aléatoires, un circuit de cryptage 7 pour crypter des données, un dispositif de contact ou connecteur 9 pour établir la communication avec un terminal 21 (qu'on décrira ultérieurement), et un élément de commande 11 tel qu'une unité centrale de traitement (UC) pour commander les éléments précités. La mémoire 3, le générateur de nombres aléatoires 5 et l'élément de commande 11 sont intégrés par exemple dans une puce de

circuit intégré (ou plusieurs puces de circuit intégré), et ils sont noyés dans l'épaisseur de la carte de paiement.

La mémoire 3 est constituée par une mémoire non volatile telle qu'une mémoire EEPROM (mémoire morte programmable électriquement effaçable), et elle est divisée en une table de définition de zones 13 et en un fichier de données 15, comme le montre la figure 2. Le fichier de données 15 est divisé en un ensemble de zones 17. Les zones 17 sont respectivement définies par des données de définition de zones 19 qui se trouvent dans la table de définition de zones 13.

Les données de définition de zones 19 consistent en une chaîne de données dans laquelle un numéro de zone (AID), constituant des données d'identification pour désigner une zone, des données d'adresse de début de la mémoire qui correspondent à une zone, des données de taille pour définir la capacité d'une zone, et des données d'attribut, sont incorporées de façon mutuellement correspondante. Chaque donnée d'attribut comprend par exemple un multiplet. Si le bit de plus fort poids (ou MSB) de données d'attribut est "0", il represente une zone d'écriture de données cryptées. Si le bit de plus fort poids est égal à "1", il représente une zone d'écriture de données d'entrée.

Le terminal (second dispositif électronique) 21 a pour fonction de traiter la carte de paiement 1. Le terminal 21 comprend une mémoire 23 pour enregistrer diverses données, un générateur de nombres aléatoires 25 pour produire des données de nombres aléatoires, un circuit de cryptage 27 pour crypter des données, un clavier 29 pour introduire des données, un dispositif de visualisation 31 pour visualiser des données, un dispositif de contact ou connecteur 33 pour communiquer avec la carte de paiement 1, un con-

trôleur de communication 35 pour réaliser une communication en temps réel faisant intervenir un centre de traitement (ordinateur hôte) 39 et une ligne de communication 41, et une section de commande 37, telle qu'une unité centrale, pour commander les éléments précités.

On décrira ci-après en détail un système et un procédé de vérification conformes à l'invention, en se référant aux figures 3A à 3C. On suppose qu'une liste de données de clé et une liste de numéros de données de clé (KID), qui sont représentées sur la figure 3A, sont enregistrées dans la mémoire 23 du terminal 21. Une liste de données de clé est une liste dans laquelle des numéros de données de clé et des données de clé sont disposés en correspondance mutuelle. Une liste KID ne contient que des numéros de données de clé, pour désigner des données de clé. La carte de paiement 1 comporte sa propre liste de données de clé qui est enregistrée dans la mémoire 3 de la carte de paiement, lorsque cette dernière est émise.

On décrira ci-après un processus de vérification mutuelle entre la carte de paiement 1 et le terminal 21, en se référant aux étapes 43 à 57. A l'étape 43, le terminal 21 produit des données de nombres aléatoires R1 en utilisant le générateur de nombres aléatoires 25, et il les émet vers la carte de paiement 1 en utilisant un ordre de préparation de vérification EXCH. A cet instant, un numéro de données de clé KID-M concernant une donnée de clé que le terminal 21 utilise pour vérifier la carte de paiement, et des données pour désigner un algorithme de cryptage ALG qui est mis en oeuvre par le terminal 21, sont également émises vers la carte de paiement 1.

A l'étape 45, lorsque la carte de paiement 1 reçoit l'ordre de préparation de vérification EXCH, il

produit des données de nombres aléatoires R2 en utilisant le générateur de nombres aléatoires 5, et il les émet vers le terminal 21, à titre de réponse exch à l'ordre de préparation de vérification EXCH. A ce moment, la carte de paiement 1 trouve dans sa propre liste de numéros de données de clé un numéro de données de clé KID-N de la donnée de clé qui est utilisée pour la vérification du terminal 21, elle effectue un contrôle pour déterminer si le terminal est capable de mettre en oeuvre l'algorithme de cryptage désigné (ALG), et elle émet ce résultat de contrôle sous la forme de l'information "alg" vers le terminal 21, en compagnie des données de nombres aléatoires R2.

Si le numéro de données de clé KID-M qui est désigné par le terminal 21 ou le numéro de données de clé KID-N qui est utilisé par la carte de paiement 1 pour vérifier le terminal 21, n'est pas présent dans la liste de numéros de données de clé, ou si l'algorithme de cryptage désigné ne peut pas être mis en oeuvre, la carte de paiement 1 signale cette condition au terminal 21.

A l'étape 47, le terminal 21 trouve dans sa propre liste de numéros de données de clé un numéro de données de clé KID-N qui correspond à la donnée de clé de cryptage désignée par la carte de paiement 1, et il extrait la donnée de clé correspondante NNNNN. Le circuit de cryptage 7 crypte ensuite les données de nombres aléatoires R2 en utilisant la donnée de clé NNNNN conformément à l'algorithme de cryptage ALG qui est désigné par l'ordre de préparation de vérification EXCH, pour obtenir ainsi des données cryptées C2X.

A l'étape 51, la carte de paiement 1 compare les données cryptées C2X obtenues à l'étape 47 avec des données cryptées C2X figurant dans un ordre de vérification AUTH reçu précédemment, et elle détermine

un résultat de comparaison O/N.

A l'étape 53, la carte de paiement 1 extrait un numéro de données de clé MMMMM correspondant au numéro de données de clé KID-M de la donnée de clé de cryptage désignée par l'ordre de préparation de vérification EXCH, provenant du terminal 21. Le circuit de cryptage 7 crypte ensuite les données de nombres aléatoires R1 en utilisant la donnée de clé MMMMM conformément à l'algorithme de cryptage ALG, pour obtenir ainsi des données cryptées C1. La carte de paiement 1 émet vers le terminal 21 les données cryptées C1 et le résultat de comparaison O/N à l'étape 51, à titre de réponse auth à l'ordre de vérification AUTH.

A l'étape 55, lorsque le terminal 21 reçoit la réponse auth, il extrait une donnée de clé MMMMM correspondant au numéro de données de clé KID-M de la donnée de clé de cryptage émise précédemment. Le circuit de cryptage 27 crypte ensuite les données de nombres aléatoires R1 qui sont produites à l'étape 43, en utilisant la donnée de clé MMMMM conformément à l'algorithme de cryptage ALG, pour obtenir ainsi des données cryptées C1X.

A l'étape 57, le terminal 21 compare les données cryptées C1 qui sont reçues à titre de réponse auth, avec les données cryptées C1X qui sont produites à l'étape 55, et il détermine le traitement de système suivant sur la base du résultat de comparaison, ainsi que du résultat de comparaison qui est reçu à partir de la carte de paiement 1 à l'étape 51, par la réponse auth.

On décrira ci-après un processus d'écriture de données du terminal 21 vers la carte de paiement 1 et de vérification du processus d'écriture, en se référant aux étapes 59 à 87. A l'étape 59, le terminal 21 émet une demande d'écriture de données vers la car-

te de paiement en utilisant un ordre d'écriture ECRITURE, qui contient un numéro de zone AID-A d'une zone de destination de la mémoire 3 dans la carte de paiement 1, un nombre de multiplets L-1 des données à écrire, et des premières données M1-1 parmi des données à écrire M1 qui sont divisées en un ensemble de blocs de données correspondant à des multiplets, que la carte de paiement 1 peut recevoir à titre de données d'entrée. A l'étape 61, la carte de paiement 1 trouve une zone à laquelle le numéro de zone AID-A, reçu au moyen de l'ordre d'écriture ECRITURE, est ajouté à partir de la table de définition de zones 13. Si aucune zone correspondante n'est trouvée, la carte de paiement 1 émet vers le terminal 21 une information d'état représentant le fait que le numéro de zone n'est pas défini, en utilisant une réponse "écriture" à l'ordre d'écriture ECRITURE. Si une telle zone est trouvée, la carte de paiement 1 effectue un contrôle pour déterminer si l'ordre de préparation de vérification EXCH précédent ou un ordre de préparation de cryptage SRND (qu'on décrira ultérieurement) est correctement exécuté.

S'il n'est pas correctement exécuté, la carte de paiement 1 émet vers le terminal 21 une information d'état d'inachèvement de condition d'exécution, en utilisant la réponse "écriture". Si la détermination qui est faite indique qu'un ordre correspondant est correctement exécuté, la carte de paiement 1 produit des données initiales R1a sur la base des données de nombres aléatoires R1 spécifiées précédemment par l'ordre de préparation de vérification EXCH et de la valeur propre à la carte qui est conservé dans la carte de paiement 1, par exemple par une opération OU-EXCLUSIF.

A l'étape 63, la carte de paiement 1 crypte

les données à écrire M1-1 en utilisant les données initiales R1a et la donnée de clé MMMMM correspondant au numéro de données de clé KID-M qui a été notifé précédemment par l'ordre de préparation de vérification EXCH, conformément à l'algorithme de cryptage ALG désigné précédemment par l'ordre de préparation de vérification EXCH, pour obtenir ainsi les données cryptées C1-1. Dans ce mode de réalisation, le cryptage est effectué conformément au mode d'enchaînement de blocs de chiffres ou CBC ("Cypher Block Chaining"). Dans un mode de cryptage normal, le cryptage peut être effectué seulement en blocs de 8 multiplets. Par conséquent, lorsqu'on doit crypter des données d'une longueur supérieure à 8 multiplets, on divise les données en blocs de 8 multiplets, et le résultat de cryptage des premières données divisées est renvoyé pour le cryptage des données divisées suivantes. Du fait qu'on ne dispose pas d'une valeur renvoyée au moment du cryptage des premières données divisées, on utilise les données initiales R1a à titre de valeur renvoyée.

En se référant aux données d'attribut de la zone, correspondant à une destination d'accès, désignée par le numéro de zone AID-A, on détermine si les données d'entrée M1-1 ou les données cryptées C1-1 sont écrites dans la mémoire 3, et on effectue une opération d'écriture. Ensuite, la carte de paiement 1 émet une réponse nb vers le terminal 1 pour demander les données à écrire suivantes.

A la réception de la réponse nb, le terminal 21 émet vers la carte de paiement 1 les données à écrire suivantes M1-2, à l'étape 65. A l'étape 67, lorsque la carte de paiement 1 reçoit les données à écrire suivantes M1-2, elle crypte les données à écrire M1-2 en utilisant les dernières données à 8 multiplets des données cryptées C1-1 qui ont été produites

précédemment, et la donnée de clé MMMMM correspondant au numéro de données de clé KID-M, conformément à l'algorithme de cryptage ALG, pour obtenir ainsi les données cryptées C1-2. Les dernières données à 8 multiplets sont utilisées dans ce cas, du fait que le cryptage est effectué dans le mode CBC, et le résultat du cryptage des premières données à 8 multiplets est incorporé dans les dernières données à 8 multiplets. De façon similaire à l'étape 63, on détermine si les données d'entrée M1-2 ou les données cryptées C1-2 sont écrites dans la mémoire 3, et on écrit sélectivement des données correspondantes dans la zone. Ensuite, la carte de paiement 1 émet une réponse "nb" vers le terminal 21, pour demander les données à écrire suivantes.

On répète ensuite une opération identique à celle des étapes 65 et 67.

Lorsqu'à l'étape 69 le terminal 21 émet vers la carte de paiement 1 les dernières données M1-n parmi les données divisées, la carte de paiement 1 effectue une opération identique à celle décrite ci-dessus à l'étape 71. Comme décrit ci-dessus, du fait que le résultat du cryptage des premières données à 8 multiplets est incorporé dans les dernières données, on peut vérifier toutes les données en émettant les dernières données. La carte de paiement 1 émet les dernières données à 8 multiplets des dernières données cryptées C1-n, à titre de données de vérification AC1, vers le terminal 21, au moyen d'une réponse "écriture" à l'ordre d'écriture ECRITURE.

Autrement dit, dans l'opération décrite ci-dessus, dans le but de vérifier la carte de paiement 1 conformément à la procédure de vérification mutuelle, le terminal 21 obtient au préalable les données de vérification AC1 relatives aux données à écrire M1, en utilisant la donnée de clé MMMMM pour désigner la car-

te de paiement 1, l'algorithme de cryptage ALG et les données de nombres aléatoires R1.

On décrira ci-après en se référant aux étapes 73 à 81 un processus pour obtenir des données de vérification en utilisant des données de clé, un algorithme de cryptage et des données aléatoires qui diffèrent de ceux du mode de réalisation ci-dessus. A l'étape 73, le terminal 21 produit de nouvelles données aléatoires R3 en utilisant le générateur de nombres aléatoires 25, et il les émet vers la carte de paiement 1, sous la forme d'un ordre de préparation de cryptage SRND, avec un numéro de données de clé KID-A correspondant à une donnée de clé qui est utilisée par la carte de paiement 1 pour produire des données de vérification, et d'un algorithme de cryptage ALGa.

A l'étape 75, lorsque la carte de paiement 1 reçoit l'ordre de préparation de cryptage SRND, elle trouve un numéro de données de clé KID-A dans sa propre liste de clés, de façon à obtenir une donnée de clé correspondante AAAAA, et elle émet une réponse SRND vers le terminal 21.

A l'étape 77, le terminal 21 émet une demande d'écriture de données vers la carte de paiement 1, en utilisant un ordre d'écriture ECRITURE. A ce moment le terminal 21 émet un numéro de zone AID-B d'une zone de destination de la mémoire 3 dans la carte de paiement 1, un nombre de multiplets L-2 de données à écrire, et des données à écrire M2. On note qu'à l'étape 77 le nombre de multiplets des données à écrire M2 est un nombre de multiplets qui peut être reçu par la carte de paiement 1 sous la forme de données d'entrée.

A l'étape 79, la carte de paiement 1 trouve une zone à laquelle est annexé le numéro de zone AID-B dans la table de définition de zone 13 de la figure 2, de la même manière qu'à l'étape 61. Si l'ordre de pré-

paration de cryptage SRND précédent (ou l'ordre de préparation de vérification EXCH) est correctement exécuté, la carte de paiement 1 produit des données initiales R3a sur la base des données aléatoires R3 qui sont notifiées par l'ordre de préparation de cryptage SRND, et de la valeur spécifique à la carte qui est conservée dans la carte de paiement 1. A l'étape 81, la carte de paiement 1 crypte les données à écrire N2 en utilisant les données initiales R3a et la donnée de clé AAAAA correspondant au numéro de données de clé KID-A qui a été notifié précédemment par l'ordre de préparation de cryptage SRND, conformément à l'algorithme de cryptage désigné précédemment par l'ordre de préparation de cryptage SRND, pour obtenir ainsi les données cryptées C2. En se référant aux données d'attribut de la zone, constituant une destination d'accès, qui est désignée par le numéro de zone AID-B, on détermine si les données d'entrée M2 ou les données cryptées C2 sont écrites dans la mémoire 3, et on effectue une opération d'écriture. Ensuite, la carte de paiement 1 émet vers le terminal 21 les dernières données à 8 multiplets des données cryptées C2, à titre de données de vérification AC2, en utilisant une réponse "écriture" à l'ordre d'écriture ECRITURE.

On note que la carte de paiement 1 reconnaît la position physique d'une zone de destination dans la mémoire 3 conformément à des données d'adresse de début et des données de taille qui figurent dans la table de définition de zones 13 de la figure 2. Les données d'adresse de début constituent la valeur d'adresse de début de la zone correspondante, et les données de taille définissent la capacité de la zone à partir de la valeur d'adresse de début. De plus, les données d'attribut comprennent un multiplet. Si le bit de moindre poids des données d'attribut est "0", il re-

présente une zone décriture de données cryptées. S'il est égal à "1", il représente une zone d'écriture de données d'entrée.

A l'étape 83, lorsque l'opération d'écriture de données dans la carte de paiement 1 est terminée, le terminal 21 prépare une liste de traitement d'écriture de données sur la base des données de nombres aléatoires R1 et R3 correspondant aux données à écrire M1 et M2, des numéros de données de clé KID-M et KID-A, des données de vérification AC1 et AC2, et des valeurs de désignation d'algorithme ALG et ALGa. La liste préparée est ensuite émise vers le centre de traitement 39.

A l'étape 85, à la réception de la liste provenant du terminal 21, le centre de traitement 39 extrait de la liste les données à écrire M1, il trouve dans sa propre liste de clés une donnée de clé MMMMM, en utilisant le numéro de données de clé KID-M correspondant, et il produit des données de vérification AC1X sur la base des données de nombres aléatoires R1 et de l'algorithme de cryptage ALG correspondants, dans sa propre liste de transactions.

A l'étape 87, le centre de traitement 39 compare des données de vérification correspondantes AC1 dans sa propre liste avec les données de vérification AC1X qui sont produites à l'étape 85. Si ces données coïncident mutuellement, le centre de traitement 39 vérifie l'opération d'écriture pour les données à écrire M1.

Des opérations d'écriture pour des données faisant suite aux données à écrire M2 sont vérifiées de la même maniée qu'aux étapes 85 et 87.

On va maintenant décrire le fonctionnement de la carte de paiement en se référant aux figures 4A à 4GN.

Après que l'unité centrale 11 a été mise sous tension par un signal de commande provenant de la borne 21, elle émet vers le terminal 21, à l'étape 91, des données de réponse initiales appelées "réponse à la restauration". A l'étape 93, l'unité centrale 11 restaure un indicateur d'exécution d'ordre de préparation de vérification et un indicateur d'exécution d'ordre de préparation de cryptage, et elle est placée dans un état d'attente à l'étape 95.

Si l'unité centrale 11 reçoit des données d'instruction à l'étape 95, elle effectue à l'étape 97 un contrôle visant à déterminer si les données d'instruction sont l'ordre de préparation de vérification EXCH qui est représenté sur la figure 5. Si la réponse est NON à l'étape 97, la séquence passe à l'étape 131.

Si la réponse est OUI à l'étape 97, l'unité centrale 11 prélève le contenu d'un champ de numéro de données de clé (KID) dans l'ordre de préparation de vérification, et à l'étape 99 elle trouve un numéro de données de clé identique dans la liste de clés qui est enregistrée dans la mémoire 3.

Si le numéro de données de clé n'est pas trouvé à l'étape 101, l'unité centrale 11 émet à l'étape 103 une information d'état d'erreur de désignation de données de clé, et elle retourne à l'état d'attente. Si le numéro de données de clé est trouvé, l'unité centrale 11 sauvegarde la donnée de clé correspondante dans un premier tampon de clé dans la mémoire vive interne, à l'étape 105.

A l'étape 107, l'unité centrale 11 examine un champ de données de désignation d'algorithme de cryptage ALG dans l'ordre de préparation de vérification, de façon à contrôler la présence/absence d'un algorithme de cryptage enregistré dans la mémoire. Si l'unité centrale détermine à l'étape 109 qu'aucun al-

gorithme de cryptage enregistré n'est présent, elle émet à l'étape 111 une information d'état d'erreur d'algorithme désigné, et elle retourne à l'état d'attente à l'étape 95.

Si la réponse à l'étape 109 est OUI, l'unité centrale 11 sauvegarde le numéro de l'algorithme de cryptage à l'étape 113.

A l'étape 115, l'unité centrale 11 sauvegarde le nombre aléatoire R1 de l'ordre de préparation de vérification, et elle cherche ensuite dans la liste de clés un numéro de données de clé KIDa correspondant à la donnée de clé de vérification de la carte de paiement. Si le numéro de données de clé n'est pas trouvé à l'étape 119, l'unité centrale 11 émet à l'étape 121 une information d'état d'erreur de donnée de clé non enregistrée, et elle retourne à l'état d'attente. Si le numéro de données de clé est trouvé à l'étape 119, l'unité centrale 11 sauvegarde la donnée de clé correspondante dans un second tampon de clé dans la mémoire vive interne, à l'étape 123.

A l'étape 125, l'unité centrale 11 produit des données de nombre aléatoire R2, en utilisant le générateur de nombres aléatoires 5, et elle les sauvegarde dans un second tampon de nombre aléatoire dans la mémoire vive interne. A l'étape 127, l'unité centrale 11 instaure l'indicateur d'exécution d'ordre de préparation de vérification. A l'étape 129, l'unité centrale 11 émet les données de nombre aléatoire R2, à titre de réponse exch, à l'ordre de préparation de vérification, vers le terminal 21, conjointement au numéro de données de clé KIDa et au contenu du champ de données de désignation d'algorithme de cryptage ALG, dans l'ordre de préparation de vérification. L'unité centrale 11 retourne ensuite à l'état d'attente à l'étape 95.

Si la réponse à l'étape 97 est NON, l'unité centrale 11 effectue un contrôle à l'étape 131 pour déterminer si l'ordre est l'ordre de vérification AUTH qui est représenté sur la figure 6. Si la réponse à l'étape 131 est NON, la séquence passe à l'étape 151.

Si la réponse à l'étape 131 est OUI, l'unité centrale 11 effectue un contrôle à l'étape 133 pour déterminer si l'indicateur d'exécution d'ordre de préparation de vérification est instauré. Si la réponse à l'étape 133 est NON, l'unité centrale 11 émet une information d'état d'erreur de non-établissement de condition d'exécution à l'étape 135, et elle retourne à l'état d'attente à l'étape 95.

Si la réponse à l'étape 133 est OUI, l'unité centrale 11 commande au circuit de cryptage 7 de crypter le contenu du second tampon de nombre aléatoire, en utilisant le contenu du second tampon de clé à titre de donnée de clé de cryptage à l'étape 137. Dans ce cas, on utilise un algorithme de cryptage correspondant au numéro d'algorithme de cryptage qui a été enregistré.

A l'étape 139, l'unité centrale 11 compare le résultat du cryptage avec des données d'entrée dans l'ordre de vérification AUTH, et elle instaure ou restaure un indicateur de coïncidence conformément au résultat de la comparaison, à l'étape 141 ou 145.

A l'étape 147, l'unité centrale 11 commande au circuit de cryptage 7 de crypter le contenu du premier tampon de nombre aléatoire, en utilisant à titre de donnée de clé de cryptage le contenu du premier tampon de clé. Dans ce cas, l'algorithme de cryptage qui est utilisé est le même qu'à l'étape 137. A l'étape 149, l'unité centrale 11 émet vers le terminal 21 le résultat crypté, sous la forme d'une réponse auth à l'ordre de vérification AUTH, en compagnie du contenu

de l'indicateur de coïncidence, et elle retourne à l'état d'attente à l'étape 95.

Si la réponse à l'étape 131 est NON, l'unité centrale 11 effectue un contrôle à l'étape 151 pour déterminer si l'ordre est l'ordre de préparation de cryptage SRND qui est représenté sur la figure 7. Si la réponse à l'étape 151 est NON, la séquence passe à l'étape 175.

Si la réponse à l'étape 151 est OUI, l'unité centrale 11 prélève le contenu d'un champ de numéro de données de clé KID dans l'ordre de préparation de cryptage, et à l'étape 153 elle cherche un numéro de données de clé identique dans la liste de clés qui est enregistrée dans la mémoire 3.

Si le numéro de données de clé n'est pas trouvé à l'étape 155, l'unité centrale 11 émet à l'étape 157 une information d'état d'erreur de désignation de données de clé, et elle retourne à l'état d'attente. Si le numéro de données de clé est trouvé à l'étape 155, l'unité centrale 11 enregistre des données de clé correspondantes dans le premier tampon de clé dans la mémoire vive interne, à l'étape 159.

A l'étape 161, l'unité centrale 11 examine un champ de données de désignation d'algorithme de cryptage (ALG) dans l'ordre de préparation de cryptage, de façon à déterminer la présence/absence d'un algorithme de cryptage enregistré dans la mémoire. Si l'unité centrale détermine à l'étape 163 qu'aucun algorithme de cryptage enregistré n'est présent, elle émet à l'étape 165 une information d'état d'erreur d'algorithme désigné, et elle retourne à l'état d'attente. Si l'unité centrale détermine à l'étape 163 qu'un algorithme de cryptage enregistré est présent, elle enregistre le numéro de l'algorithme de cryptage à l'étape 167.

A l'étape 169, l'unité centrale 11 enregistre les données de nombre aléatoire R3 de l'ordre de préparation de cryptage dans le premier tampon de nombre aléatoire dans la mémoire vive interne. A l'étape 171, l'unité centrale 11 instaure l'indicateur d'exécution d'ordre de préparation de cryptage. A l'étape 173, l'unité centrale 11 émet vers le terminal 21 une information d'état d'exécution d'ordre de préparation de cryptage, et elle retourne à l'état d'attente à l'étape 95.

Si la réponse à l'étape 151 est NON, l'unité centrale 11 effectue un contrôle à l'étape 175 pour déterminer si l'ordre est l'ordre d'écriture ECRITURE qui est représenté sur la figure 8A ou 8B. Si la réponse à l'étape 175 est NON, l'unité centrale 11 effectue un contrôle pour déterminer si l'ordre est par exemple un ordre de lecture, et elle progresse jusqu'à une étape correspondante. Si la réponse à l'étape 175 est OUI, l'unité centrale 11 effectue un contrôle à l'étape 177 pour déterminer si l'ordre d'écriture a un format représenté sur la figure 8A ou 8B. S'il a le format qui est représenté sur la figure 8A, l'unité centrale 11 examine l'indicateur d'exécution d'ordre de préparation de vérification ou l'indicateur d'exécution d'ordre de préparation de cryptage à l'étape 179. L'unité centrale 11 effectue ensuite un contrôle à l'étape 181 pour déterminer si l'un des indicateurs est instauré. Si la réponse à l'étape 181 est NON, l'unité centrale 11 émet une information d'état de non-établissement de condition à l'étape 183, et elle retourne à l'état d'attente. Si la réponse à l'étape 181 est OUI, l'unité centrale 11 enregistre le contenu de la partie de données de l'ordre d'écriture dans un second tampon d'écriture de la mémoire vive, à l'étape 185.

Si on détermine à l'étape 177 que l'ordre d'écriture a le format qui est représenté sur la figure 8B, l'unité centrale 11 effectue un contrôle à l'étape 187 pour déterminer si un indicateur de continuation d'ordre d'écriture qui est conservé dans l'unité centrale est instauré. Si la réponse à l'étape 187 est NON, l'unité centrale 11 émet une information d'état d'erreur de demande à l'étape 189, et elle retourne à l'état d'attente à l'étape 95. Si la réponse à l'étape 187 est OUI, l'unité centrale 11 annexe le contenu (données d'entrée) de la partie de données de l'ordre d'écriture au contenu d'un tampon d'enregistrement de données dans la mémoire vive interne, et elle l'enregistre dans le second tampon d'écriture dans la mémoire vive interne à l'étape 191.

A l'étape 193, l'unité centrale 11 enregistre seulement le contenu (données d'entrée) de la partie de données de l'ordre d'écriture dans un premier tampon d'écriture dans la mémoire vive interne.

A l'étape 195, l'unité centrale 11 effectue un contrôle pour déterminer si des données suivantes à écrire sont présentes dans les données d'entrée qui sont émises en utilisant l'ordre d'écriture représenté sur la figure 8A ou 8B. Si la réponse à l'étape 195 est OUI, l'unité centrale 11 instaure un indicateur de continuation à l'étape 197. Si la réponse à l'étape 195 est NON, l'unité centrale 11 restaure l'indicateur de continuation à l'étape 199.

A l'étape 201, l'unité centrale 11 effectue un contrôle pour déterminer si le nombre de multiplets dans le second tampon d'écriture dans la mémoire vive interne est par exemple un multiple de 8. Si la réponse à l'étape 201 est OUI, la séquence passe à l'étape 203. Si la réponse à l'étape 201 est NON, l'unité centrale 11 accomplit un traitement de remplissage pour

les données qui se trouvent dans le second tampon d'écriture dans la mémoire vive interne (par exemple en ajoutant des données "20" (en hexadécimal) à la fin des données), afin de produire des données correspondant à un multiple de 8, à l'étape 205, et la séquence passe à l'étape 213.

Si la réponse à l'étape 203 est OUI, l'unité centrale 11 laisse les données correspondant à un multiple de 8, et elle sauvegarde le reste des données dans le tampon de sauvegarde de données dans la mémoire vive interne, à l'étape 209. Ainsi, si 18 multiplets de données sont présents dans le second tampon d'écriture, 16 multiplets de données seulement sont laissés, tandis que les 2 multiplets de données restants sont sauvegardés dans le tampon de sauvegarde de données. Si on détermine à l'étape 209 que le second tampon d'écriture dans la mémoire vive interne est vide, la séquence passe à l'étape 213.

Si le second tampon d'écriture dans la mémoire vive interne est vide à l'étape 209 (par exemple si 7 multiplets de données sont enregistrés dans le second tampon d'écriture , toutes les données dans le tampon sont transférées vers le tampon de sauvegarde de données; il en résulte que le second tampon d'écriture devient vide), l'unité centrale 11 effectue un contrôle à l'étape 211 pour déterminer si la zone sur laquelle porte l'accès au moment présent doit être cryptée pendant une opération d'écriture. Si la réponse à l'étape 211 est NON, la séquence passe à l'étape 215. Si la réponse à l'étape 211 est OUI, la séquence passe à l'étape 213.

A l'étape 213, l'unité centrale 11 commande au circuit de cryptage 7 de crypter les données dans le second tampon d'écriture dans la mémoire vive interne, conformément au mode CBC. Si l'indicateur de

continuation est restauré dans ce cas, une valeur obtenue par la combinaison par une fonction OU-EXCLUSIF du contenu du premier tampon de nombre aléatoire dans la mémoire interne et de la valeur spécifique à la carte, est utilisée à titre de valeur initiale pour l'opération de cryptage utilisant le mode CBC. Si l'indicateur de continuation est instauré, les 8 derniers multiplets des données cryptées dans l'opération d'écriture précédente sont utilisés à titre de valeur initiale. De plus, dans ce cas, le contenu du premier tampon de clé est utilisé à titre de donnée de clé, et un algorithme de cryptage est utilisé sélectivement conformément à un numéro d'algorithme de cryptage qui est conservé. Lorsque cette opération est terminée, la séquence passe à l'étape 215.

A l'étape 215, l'unité centrale 11 effectue un contrôle pour déterminer si l'indicateur de continuation est instauré. Si la réponse à l'étape 215 est NON, l'unité centrale 11 effectue un contrôle à l'étape 217 pour déterminer si la zone de destination de l'accès est une zone à crypter. Si la réponse à l'étape 217 est NON, l'unité centrale 11 ajoute un nombre de multiplets LX des données à écrire dans l'ordre d'écriture, au contenu du premier tampon d'écriture dans la mémoire vive interne, et elle l'écrit dans la zone de destination de l'opération d'accès dans la mémoire 3, à l'étape 219. Si la réponse à l'étape 217, est OUI, l'unité centrale 11 fixe à titre de valeur LXa la valeur minimale d'un multiple de 8 supérieur au nombre de multiplets LX des données à écrire, et elle écrit cette valeur dans la zone de destination, en l'ajoutant au contenu du second tampon d'écriture à l'étape 221.

Si la réponse à l'étape 215 est OUI, l'unité centrale 11 effectue un contrôle à l'étape 223 pour

déterminer si la zone de destination de l'opération est une zone à crypter. Si la réponse à l'étape 223 est NON, l'unité centrale 11 écrit le contenu du premier tampon d'écriture de la mémoire vive interne dans la zone de destination, en l'ajoutant aux données écrites précédemment, à l'étape 225. Si la réponse à l'étape 223 est OUI, l'unité centrale 11 écrit le contenu du second tampon d'écriture de la mémoire vive interne dans la zone de destination pour l'opération d'accès, d'une manière identique à celle décrite ci-dessus, à l'étape 227.

Après que les données ont été écrites, l'unité centrale 11 effectue un contrôle à l'étape 229 pour déterminer si l'indicateur de données suivantes est instauré. Si la réponse à l'étape 229 est OUI, l'unité centrale 11 instaure l'indicateur de continuation et elle émet une réponse "nb" à l'étape 231, et elle retourne à l'état d'attente. Si la réponse à l'étape 229 est NON, l'unité centrale 11 émet les 8 derniers multiplets du contenu du second tampon d'écriture dans la mémoire vive interne et restaure l'indicateur de continuation à l'étape 233, et elle retourne à l'état d'attente.

De cette manière, une donnée de clé et un algorithme de cryptage parmi un ensemble de données de clé et un ensemble d'algorithmes de cryptage conservés dans la carte de paiement, sont désignés par le terminal, et des données à écrire sont cryptées en utilisant la donnée de clé et l'algorithme de cryptage désignés. Par conséquent, même si la carte de paiement est utilisé dans un ensemble d'applications, on peut utiliser sélectivement des données de clé de vérification et des algorithmes de cryptage pour les applications respectives, et on peut garantir la sécurité entre les applications.

Il faut noter que les données de nombre aléatoire R1 et R2 qui doivent être émises du terminal 21 vers la carte de paiement 1 peuvent avoir le même contenu à chaque opération. Cependant, si elles sont changées à chaque opération, des données cryptées différentes sont émises à condition que des opérations d'écriture soient effectuées à des instants différents, même si on utilise des données d'écriture, des données de clé et des algorithmes de cryptage identiques. La vérification des données est donc facilitée.

Dans ce cas, si par exemple un circuit d'horloge est incorporé dans le terminal 21, et si on produit des données de nombres aléatoires R1 et R3 en utilisant des données temporelles qui sont produites par le circuit d'horloge, on peut aisément obtenir des données différentes pour chaque opération.

Il va de soi que de nombreuses modifications peuvent être apportées au dispositif et au procédé décrits et représentés, sans sortir du cadre de l'invention.

REVENDICATIONS

1. Système de vérification comprenant un premier dispositif électronique (1) contenant au moins une donnée de clé, et un second dispositif électronique (21) capable d'entrer en communication avec le premier dispositif électronique, caractérisé en ce qu'il comprend : des moyens (37, 23) pour émettre du second dispositif électronique vers le premier dispositif électronique des premières données et des données de désignation pour désigner une donnée de clé pour le cryptage des premières données; des moyens (3, 11, 7) qui, lorsque le premier dispositif électronique a reçu les premières données et les données de désignation, sélectionnent une donnée de clé parmi la ou les données de clé, conformément aux données de désignation reçues, et cryptent les premières données reçues en utilisant la donnée de clé sélectionnée; et des moyens (11, 9) pour émettre vers le second dispositif électronique une partie des données cryptées, après que le premier dispositif électronique a entièrement reçu les premières données.

2. Système selon la revendication 1, caractérisé en ce qu'il comprend en outre au moins une mémoire tampon, et des moyens pour enregistrer les premières données qui sont reçues par la mémoire tampon.

3. Système selon la revendication 1, caractérisé en ce que le premier dispositif électronique (1) contient en outre au moins un algorithme de cryptage, les moyens (37, 23) destinés à émettre les données de désignation émettent du second dispositif électronique (21) vers le premier dispositif électronique (1) des premières données, des données de clé pour le cryptage des premières données et des données de désignation pour désigner un algorithme de cryptage, et les moyens (3, 11, 7) destinés à crypter les

premières données sélectionnent une donnée de clé et un algorithme de cryptage parmi la ou les données de clé et le ou les algorithmes de cryptage, conformément aux données de désignation reçues, et ils cryptent les premières données reçues en utilisant la donnée de clé et l'algorithme de cryptage sélectionnés.

4. Système selon la revendication 3, caractérisé en ce qu'il comprend en outre des moyens (35, 25) pour émettre du second dispositif électronique (21) vers le premier dispositif électronique (1) des premières données et des secondes données dont le contenu varie à chaque opération, et les moyens de cryptage des premières données cryptent les premières données en utilisant les secondes données, la donnée de clé et l'algorithme de cryptage.

5. Système selon la revendication 3, caractérisé en ce qu'il comprend en outre : des moyens (3, 11) pour émettre vers le second dispositif électronique des données qui ont été cryptées par les moyens de cryptage des premières données; des moyens (23, 27) pour vérifier le premier dispositif électronique (1) sur la base du contenu des données cryptées lorsque les données cryptées sont reçues par le second dispositif électronique; des moyens (37, 25) pour émettre les secondes données du second dispositif électronique vers le premier dispositif électronique; des moyens (3, 11, 7) qui, lorsque les secondes données sont reçues par le premier dispositif électronique, cryptent les secondes données reçues en utilisant la donnée de clé et l'algorithme de cryptage sélectionnés sur la base des données de désignation; et des moyens (3, 11) pour émettre une partie des secondes données cryptées du premier dispositif électronique vers le second dispositif électronique.

6. Système selon l'une quelconque des reven-

dications 1 à 5, caractérisé en ce que la donnée de clé est sélectionnée conformément à une application.

7. Système selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le second dispositif électronique comprend des moyens de génération de nombres aléatoires (25) pour produire les premières données.

8. Système selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le second dispositif électronique (21) contient au moins une donnée de clé et au moins un algorithme de cryptage.

9. Système selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comprend en outre des moyens pour crypter les premières données en utilisant la donnée de clé et l'algorithme de cryptage qui sont contenus dans le second dispositif électronique (21); et des moyens pour comparer les données cryptées par le premier dispositif (1) avec les données cryptées par le second dispositif (21).

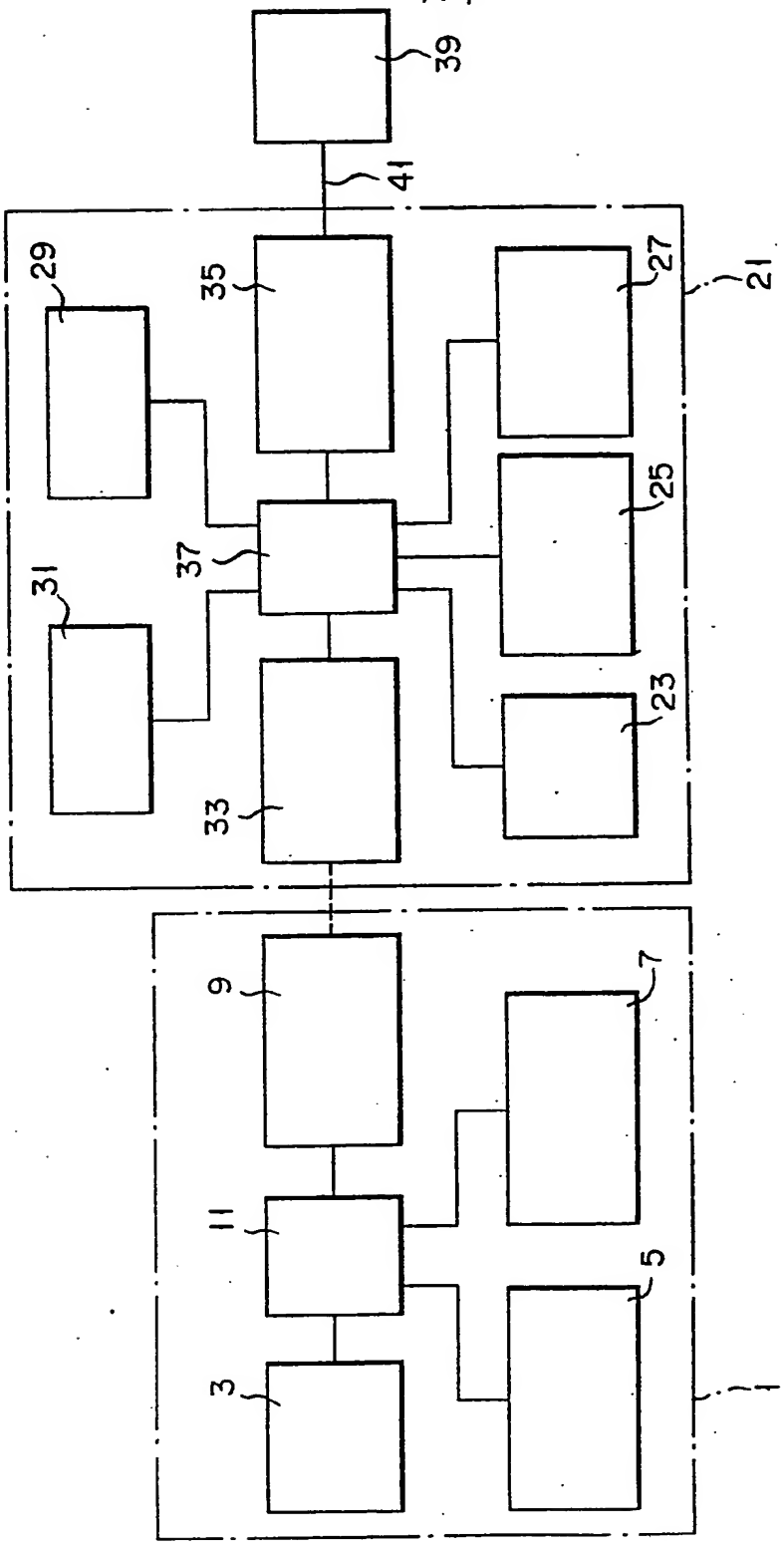


FIG. 1

Express Label No.
EV343685915US

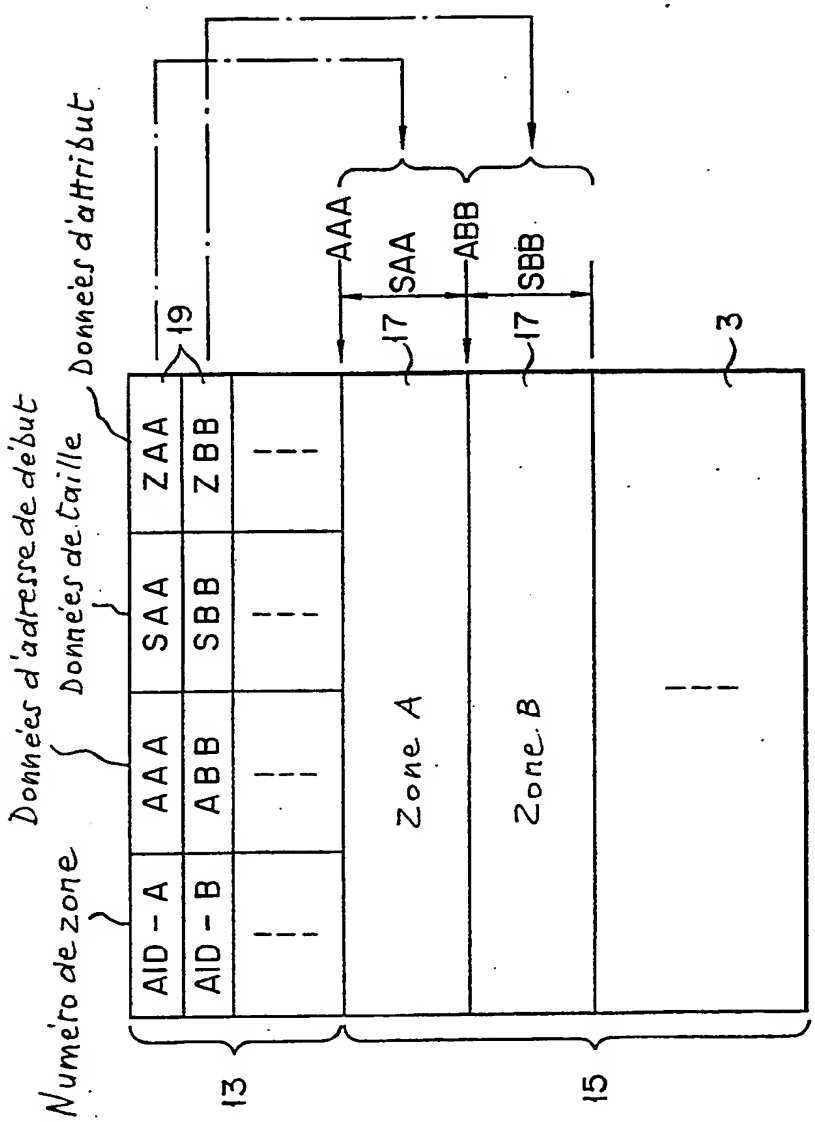


FIG. 2

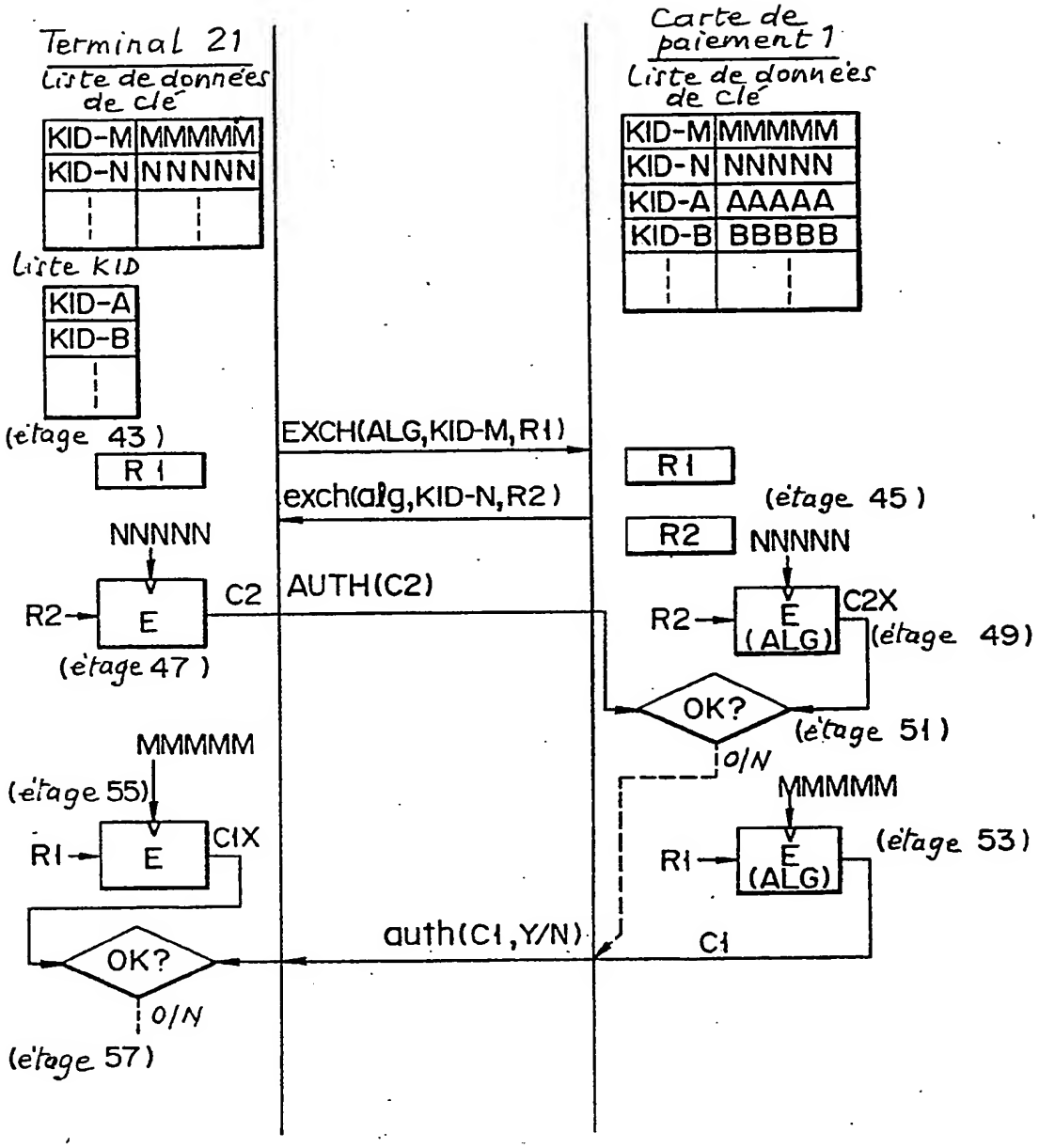
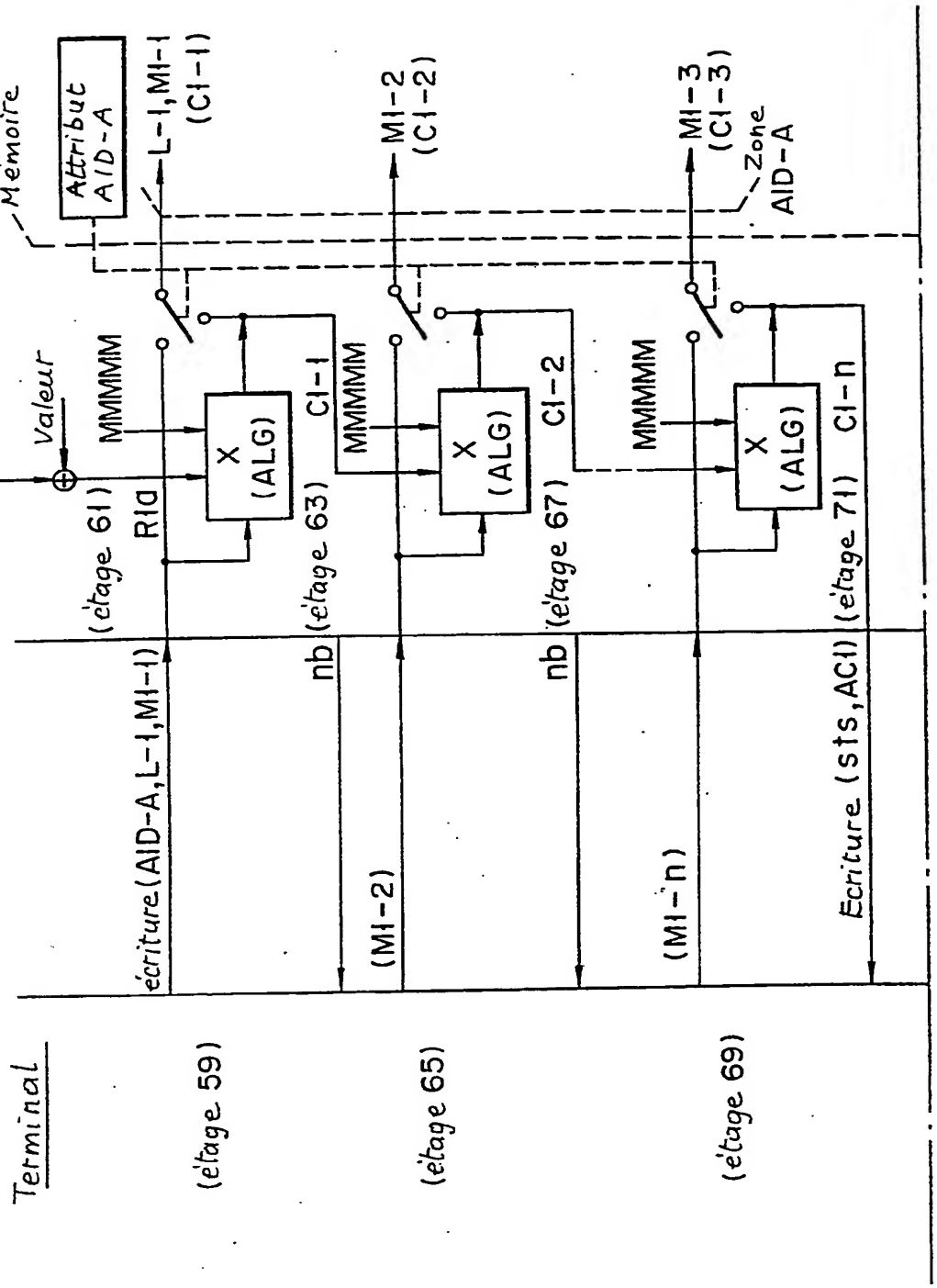


FIG. 3A

Express Label No.
EV343685915US

FIG. 3B-1



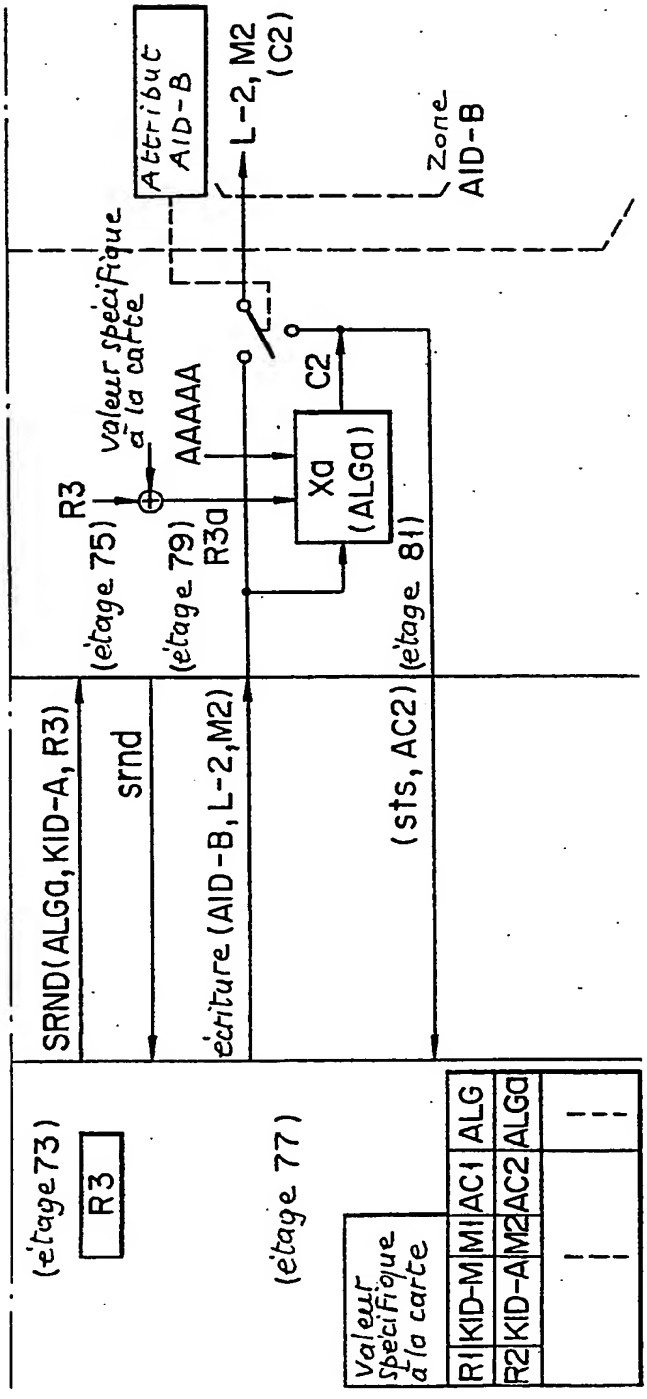


FIG. 3B-II

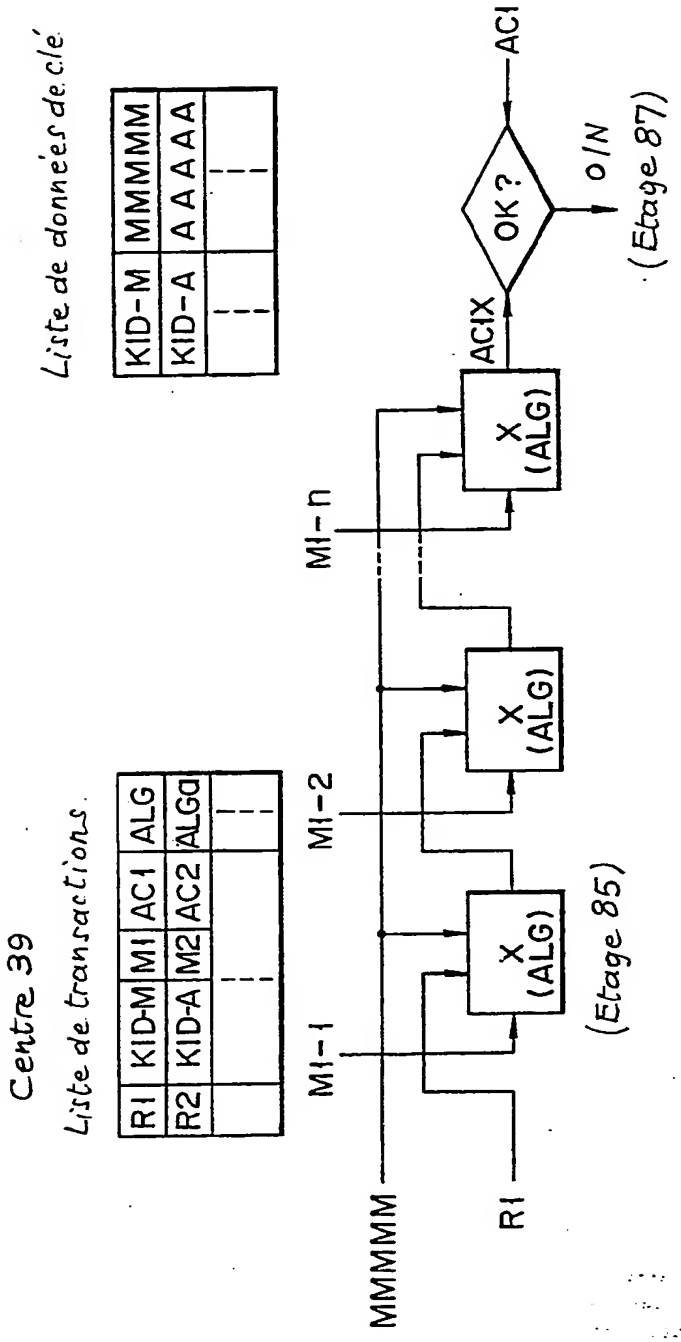


FIG. 3C

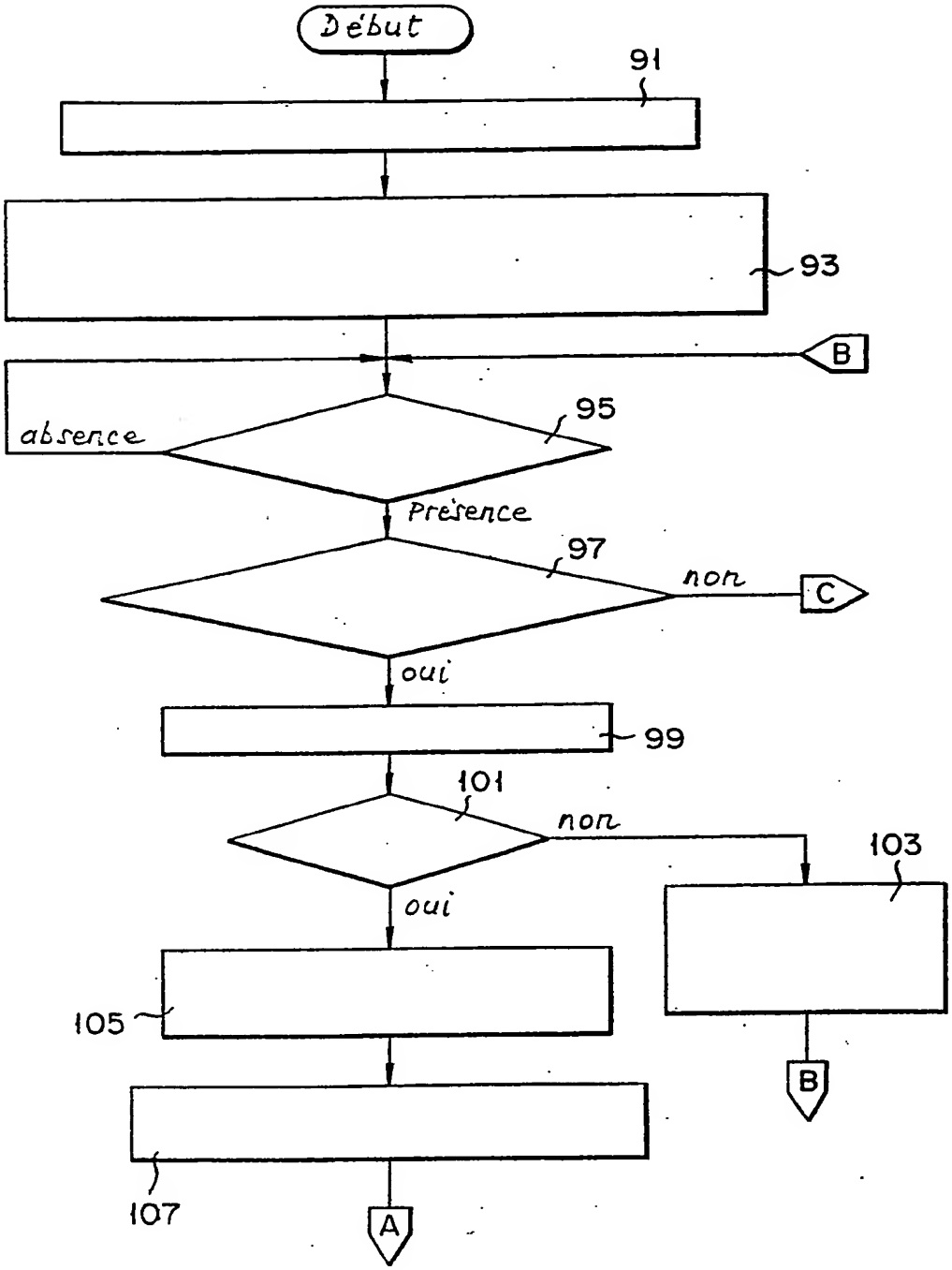


FIG. 4A

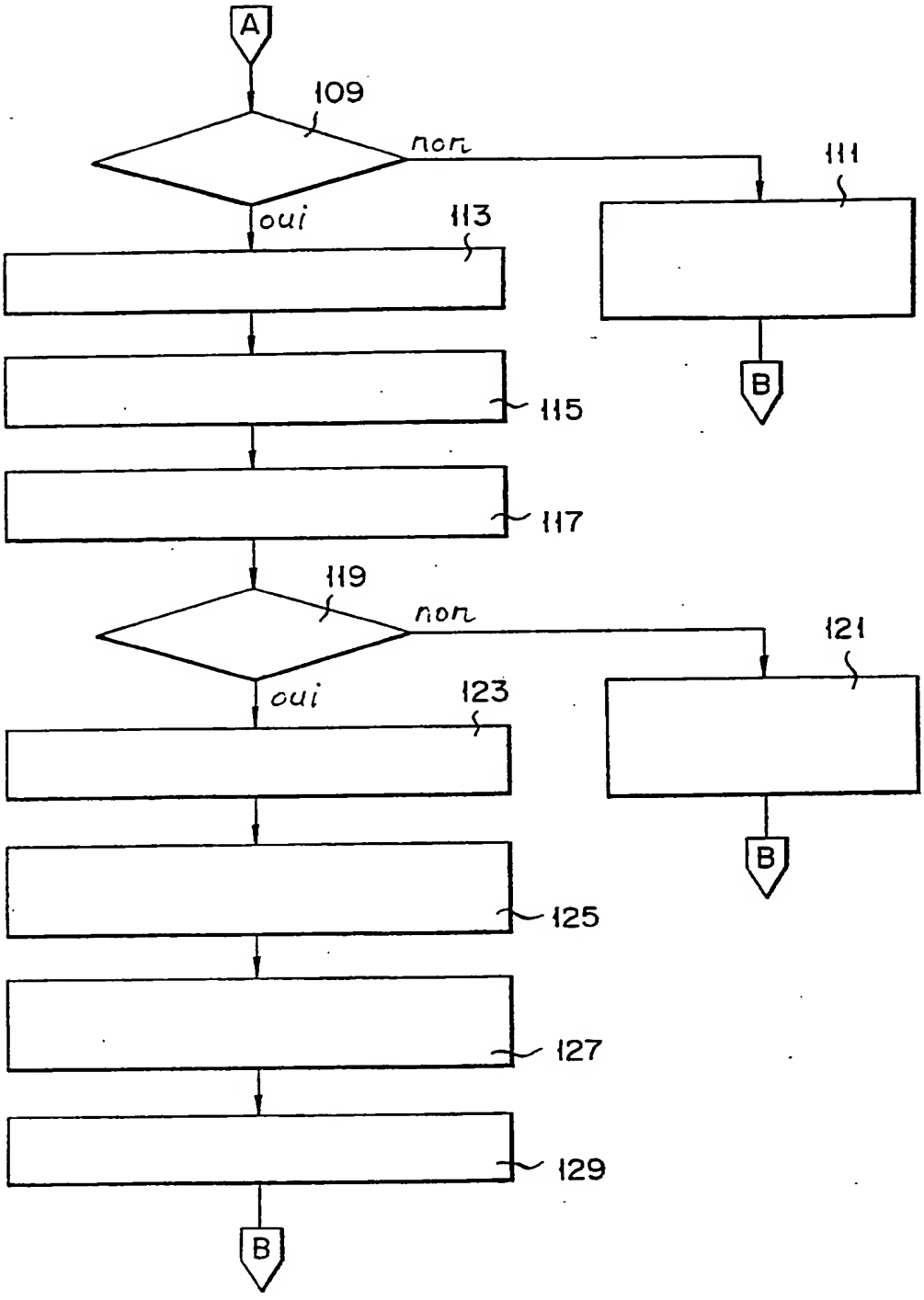


FIG. 4B

Express Label No.
EV343685915US

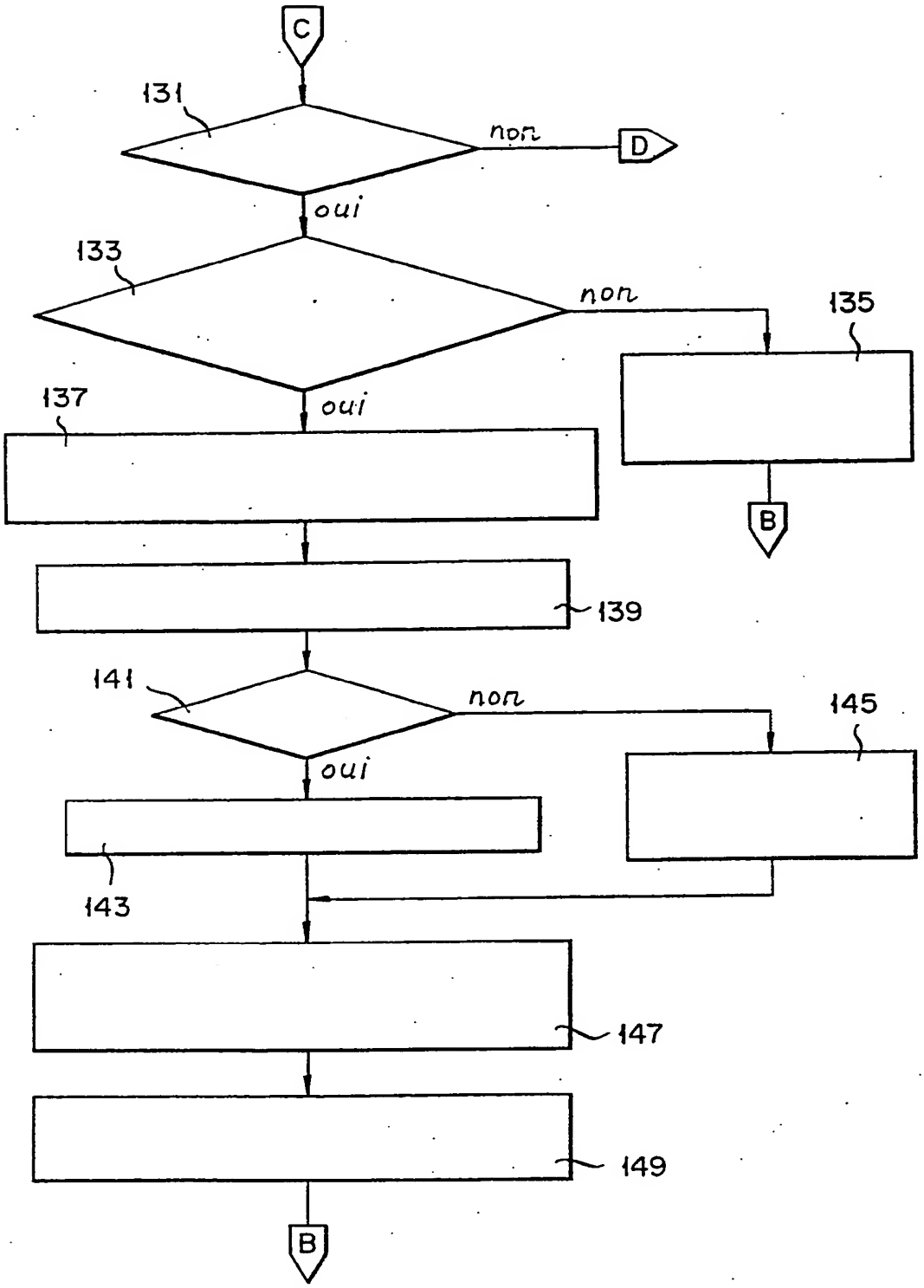


FIG. 4C

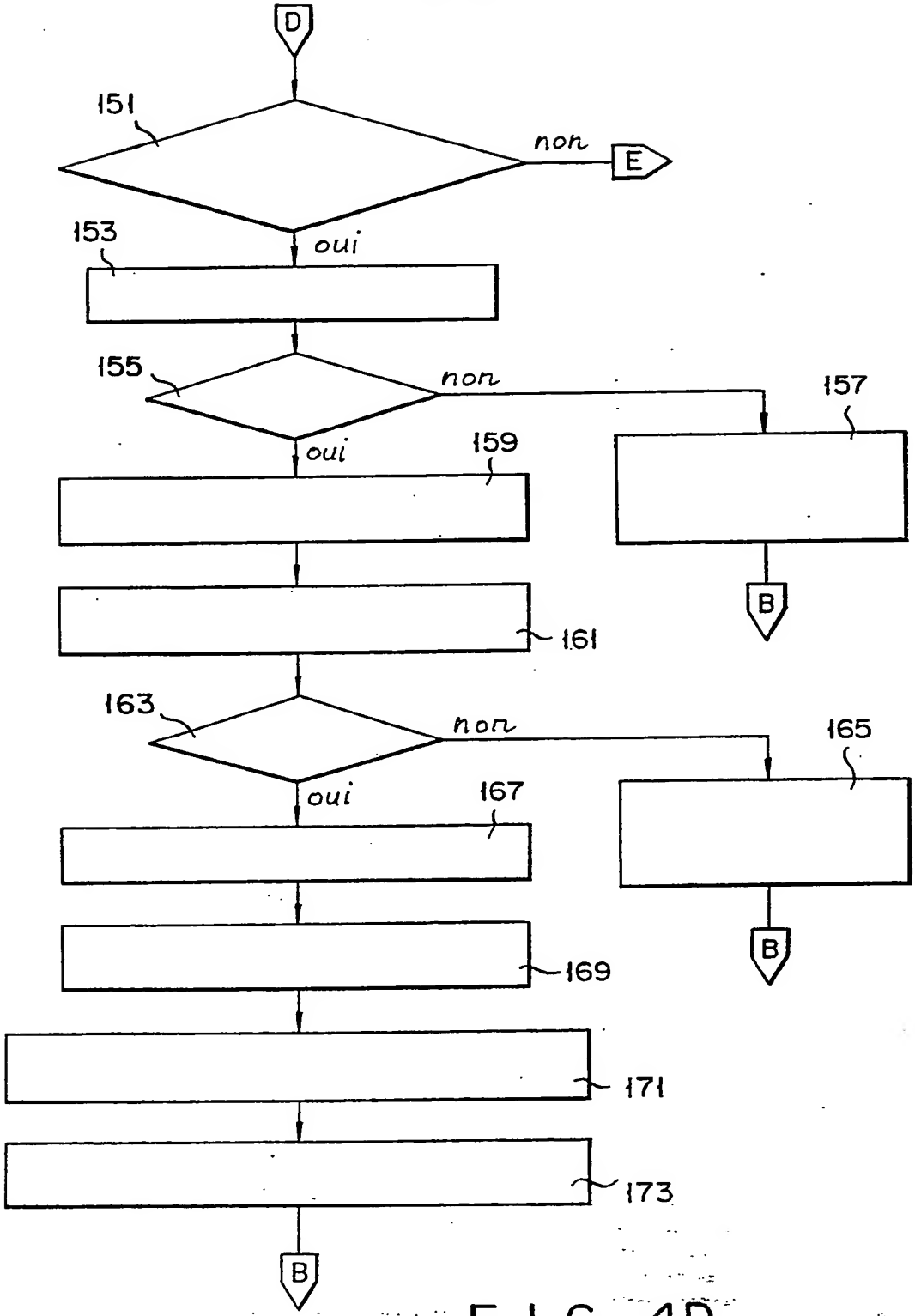


FIG. 4D

Express Label No.
EV343685915US

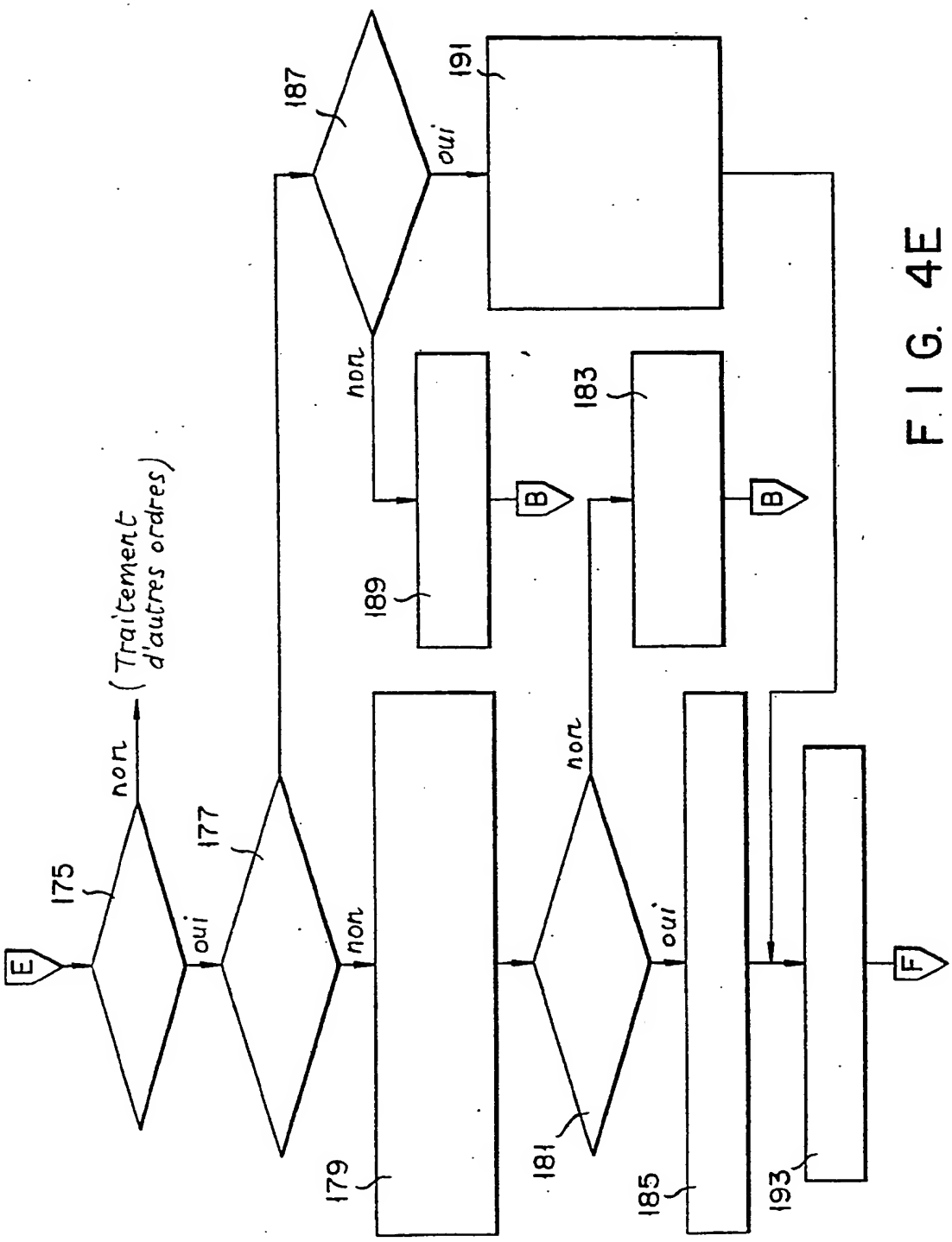


FIG. 4E

Express Label No.
EV343685915US

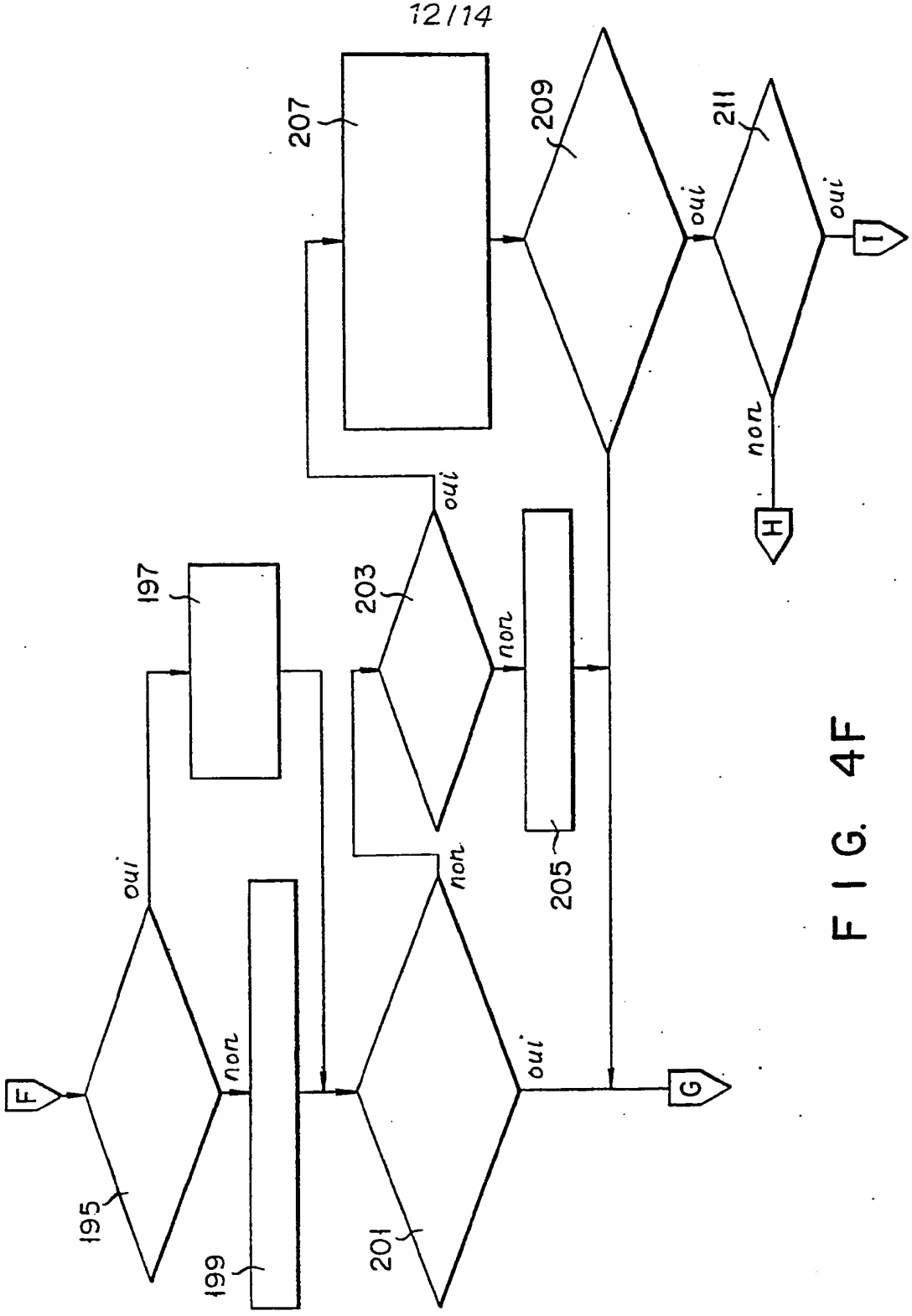


FIG. 4F

Express Label No.
EV343685915US

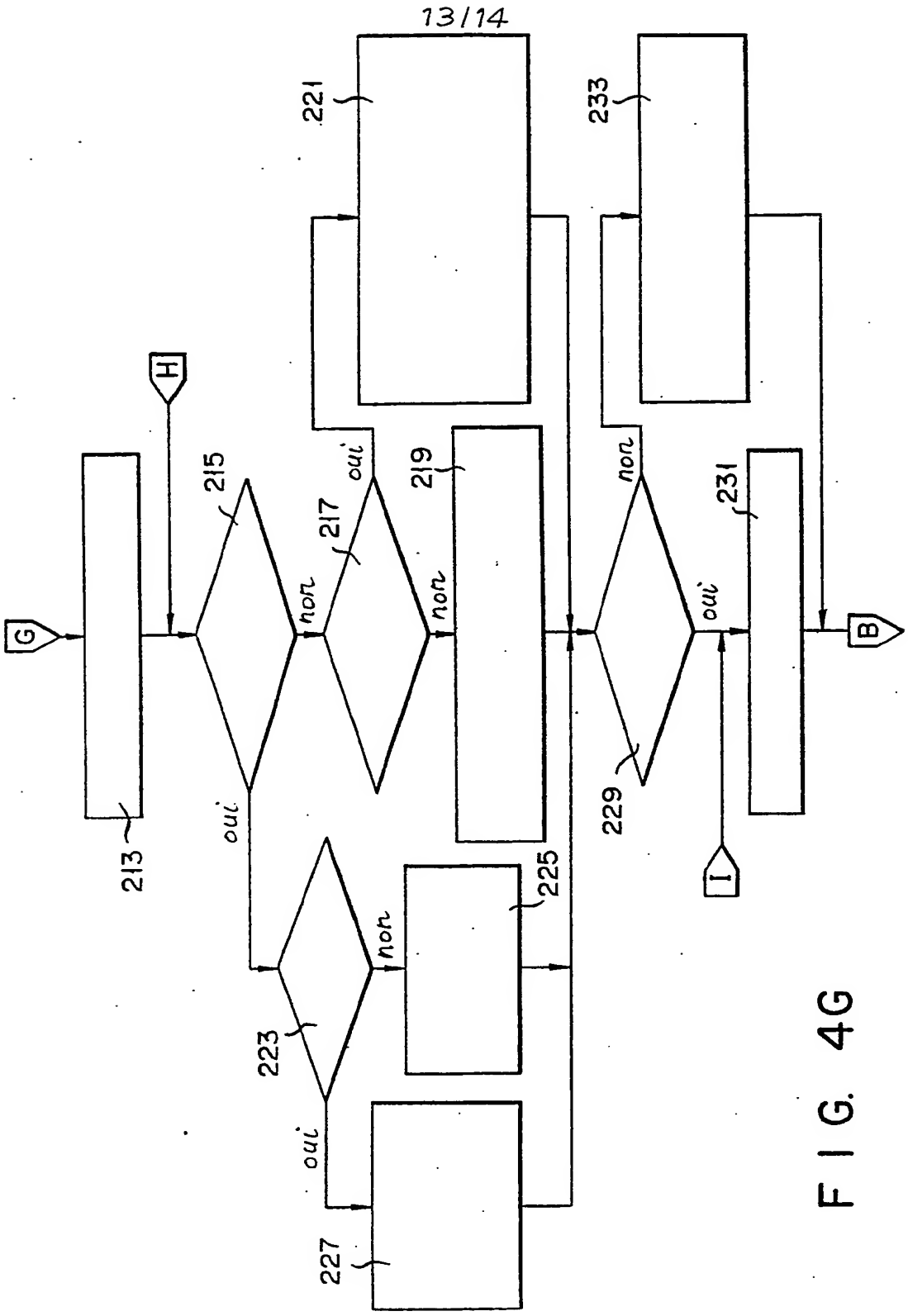


FIG. 4G

Express Label No.
EV343685915US

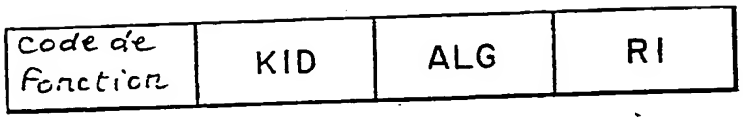


FIG. 5

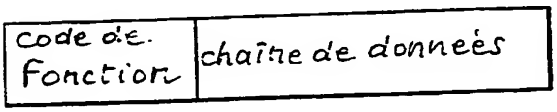


FIG. 6

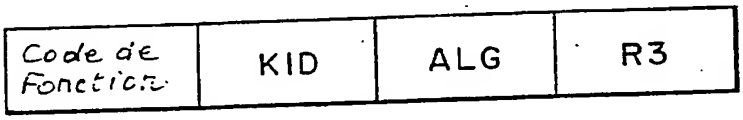


FIG. 7

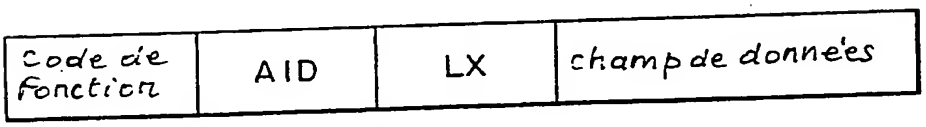


FIG. 8A

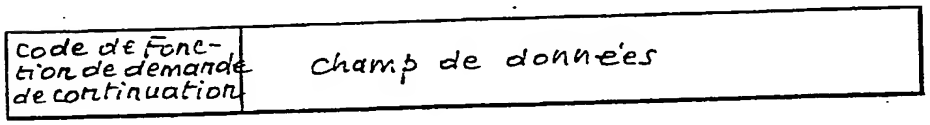


FIG. 8B